

REMARKS

Conventional digital rights management (DRM) schemes are host based in that the host, rather than the data storage engine controls the DRM process. An example of a host-based system is a personal computer surfing the Internet for digital content. Upon receipt of the content, the host includes some type of storage engine such as a hard drive to store the content. The host controls the storage engine and thus controls whatever DRM scheme is being implemented. However, hosts are inherently vulnerable to hackers.

The Ansell reference (USP 6,367,019) is a prime example of a host-based DRM scheme. Note Figure 1, which illustrates a computer system (i.e, the host) including "player" 110. As discussed in Col. 4, lines 19 through 35, in actuality this "player" is simply a collection of instructions stored in memory 104 that are implemented by processor 102. In other words, the "player" is a software process running on the host processor. It is this processor (host) that controls the DRM process. Specifically, as discussed with respect to Figures 6 and 7, an external player such as player 150 in Figure 2 may authenticate itself to host 100 so as to receive encrypted content. A "master media key" is encrypted by the host and sent to the external player, which then encrypts the master media key "and sends the encrypted master media key back to player 110." (Col. 7, lines 25-26).

As discussed with respect to step 608 of Figure 6 in Col. 7, lines 52-64, the host then writes "SPT" 116 (secure player track) to medium 202 of Figure 2. This SPT includes the encrypted content and the encrypted master media key. But note that it was the host, not the external storage engine (player 150) that controlled the creation of the encoded medium.

In sharp contrast, the storage engine recited in claim 20 features a "storage-engine" based DRM scheme. In particular, note that it is the storage engine who is configured to "to encrypt the decrypted content key with a first storage engine encryption key and to write the storage-engine-encrypted content key to the storage medium" and not the host. Thus, unlike the Ansell scheme, the storage engine encryption key never leaves the storage engine. Moreover, no host has access to this key nor does any host control the DRM process. A storage engine, unlike a host, is inherently more secure to hackers. Accordingly, Applicants respectfully submit that claim 20 is patentable over the Ansell reference.

Because claims 21 through 29 depend either directly or indirectly upon claim 20, they are patentable for at least the same reasons.

LAW OFFICES OF
THERSON, KWOK CHEN
& HEIO LLP

21 TECHNOLOGY DRIVE
SUITE 220
SAN JOSE, CA 95110
(415) 751-7040
FAX (408) 392-8262

Claim 30 is a method claim corresponding analogously to the apparatus claim of claim 20 and is thus patentable over the prior art and supported as discussed with respect to claim 20. Because claim 31 depends upon claim 30, it is patentable for at least the same reasons.


Claims 26 and 31 are cancelled, thereby mooted their rejections.

CONCLUSION


For the above reasons, pending claims 20 – 25 and 27 – 30 are in condition for allowance and allowance of the application is hereby solicited. If the Examiner has any questions or concerns, a telephone call to the undersigned at (949) 752-7040 is welcomed and encouraged.

Certification of Facsimile Transmission

I hereby certify that this paper is being facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

 June 9, 2005
Sandra L. Carr Date of Signature

Respectfully submitted,


Jonathan W. Hallman
Attorney for Applicant
Reg. No. 42,622

LAW OFFICES OF
THERSON, KWOK CHEN
& HEID LLP

61 TECHNOLOGY DRIVE
SUITE 226
SAN JOSE, CA 95110
(408) 752-7040
FAX (408) 192-9252